EXHIBIT "A"

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

HON. ELAINE L. CHAO, SECRETARY, UNITED STATES DEPARTMENT OF LABOR,	§	
Plaintiff,	§	**CASE NO. 4-05-CV-338-Y ECF**
v.	§	
ALLIED PILOTS ASSOCIATION,	§	
Defendant.	§	

BRIEF AMICUS CURIAE OF ALLIED UNION SERVICES

YONA ROZEN (State Bar No. 17358500)
Gillespie, Rozen, Watsky,
Motley & Jones, PC
3402 Oak Grove Ave., Suite 200
Dallas, Texas, 75204
Phone: (214) 720-2009
Fax: (214) 720-2291

JEFFREY B. DEMAIN, *pro hac vice application pending*
(California State Bar No. 126715)
JONATHAN WEISSGLASS, *pro hac vice application pending*
(California State Bar No. 185008)
Altshuler, Berzon, Nussbaum,
Rubin & Demain
177 Post Street, Suite 300
San Francisco, CA 94108
Phone: (415) 421-7151
Fax: (415) 362-8064

INTEREST OF AMICUS

Allied Union Services has assisted a wide variety of labor unions across the United States in conducting elections by Internet and telephone since 2000 through its BallotPoint election system. (Throughout this brief, elections conducted by Internet and telephone voting are jointly referred to as "electronic elections" or "electronic voting.") In addition, starting in 2002 and continuing to the present, the company has assisted in the representation elections performed under the auspices of the National Mediation Board, an independent federal agency created by the Railway Labor Act to facilitate labor-management relations in the railroad and airline industries. To date, the original BallotPoint system and its subsequent editions have been used in approximately 1,300 elections, including approximately 1,200 union elections and 100 National Mediation Board elections, and have processed approximately 700,000 votes. Declaration of Gerald B. Feldkamp in Support of Amicus Brief ("Feldkamp Amicus Dec."), ¶¶3-4.

Allied Union Services's business involves, among other things, supporting unions that conduct elections over the Internet. The company therefore has an interest in the present case, where the Secretary of Labor challenges certain features of the Internet voting system used to conduct an election for the Allied Pilots Association ("APA"). Although Allied Union Services did not participate or assist in the APA election, and although Allied Union Services's Internet voting system is different than the American Arbitration Association's Internet voting system before the Court, the Court's ruling may have implications for electronic voting generally and may affect Allied Union Services. Moreover, Allied Union Services has developed an expertise in electronic voting due to the large number of elections in which it has assisted and respectfully submits that its input may be useful to the Court in reaching a decision in this matter.

ARGUMENT

I. ALL ELECTION METHODS HAVE POTENTIAL TO VIOLATE BALLOT SECRECY

The Secretary of Labor challenges APA's election on the ground that the Internet system used to conduct the election was designed in such a way that it was possible for APA members to be identified with their votes. Secretary's Motion for Summary Judgment at 2; Secretary's Brief in Support of Motion for Summary Judgment at 30. In particular, the Secretary argues that "*anyone* who had access to an APA member's PIN [Personal Identification Number] and EIN [Employee Identification Number] could have logged onto the remote Internet voting system and viewed whether, and how, an APA member voted," and that several people had access to this information. Secretary's Brief at 31 (emphasis in original). The Secretary's investigation found no evidence that any person *actually* viewed how any voter voted. Because of the mere *possibility* that someone could have viewed how a voter voted, however, the Secretary concludes that there is a presumption that the outcome of the election was affected. *Id.*

It may appear from this argument that the voting medium at issue – the Internet – is uniquely situated to violate voter secrecy. But this is incorrect. *Any* election is suspect in the absence of adequate safeguards. Although the Secretary has a level of familiarity and comfort with on-site and mail-ballot elections, the Department of Labor's publication "Conducting Local Union Officer Elections" (at 37, 42) nonetheless points out that there are "common pitfalls" or mistakes that are often made in such elections that can violate ballot secrecy. (This publication is available at http://www.dol.gov/esa/regs/compliance/olms/localelec/localelec.pdf.) These two predominant methods of conducting union elections both have the potential of violating voter secrecy. For each method, the question is whether there are adequate safeguards and controls in place that are properly executed to ensure ballot secrecy.

The secrecy of mail-ballot elections can readily be compromised. Anyone could view a voter's completed ballot if the ballot is completed in the presence of others, or if it is not safeguarded prior to being mailed. Likewise, anyone could intercept a mailed ballot before it is filled out and vote in place of the intended voter. There is no observer watching what happens from the time the ballot is mailed out until it is returned. Moreover, returned ballots are typically collected in a Post Office Box for pickup after the close of the election period. Any number of Post Office employees have access to the ballots while they are awaiting pickup. It would certainly be possible to steam open the envelopes while they are being stored, or to use some other method or technology to noninvasively "read through" the envelopes containing the vote, and see how a voter voted. Because there is no other record of the mailed ballot, the postal worker could even open the envelope from the known voter, see the content of the vote, and then discard the ballot, without detection. *There is no reasonable way to quantify the potential extent of the secrecy violation in any of these examples.* Mail-ballot elections simply could not exist unless some trust is conferred on the parties involved, whether it is the voter abiding by the instruction to vote in secret, or the postal worker being left alone with the ballots, or ballot-handlers and observers being assumed to not collude to associate the name of a voter with the content of a vote.

On-site elections also present opportunities to observe how voters vote. Election observers and others have ready access to look at ballots if proper safeguards (such as voting booths) are not required to be used. *See, e.g., Marshall v. Local Union 12447, United Steelworkers*, 591 F.2d 199, 203-05 (3d Cir. 1978); *Brennan v. Local 3489, United Steelworkers*, 520 F.2d 516, 521-22 (7th Cir. 1975); *Donovan v. Local Union 887, United Rubber Workers*, 111 L.R.R.M. 2736, 2737, 1982 WL 31275 (M.D. Ga. 1982). Indeed, even if voting booths are used, there is the possibility that hidden, wireless cameras installed in the ceiling and lights could be used to watch how voters vote. If the

cameras go undetected during the election and are removed soon after the election, their presence may never be detected. In this situation as in mail ballots, *there is no reasonable way to quantify the extent of the secrecy violation.*

As these examples illustrate, inherent in even the predominant election methodologies are potential procedural weaknesses or vulnerabilities that may give rise to influencing the outcome of any given election. Indeed, all systems require some method of linking the vote with the voter in case of a challenge to the eligibility of a voter. Therefore, every election system has the same vulnerability that the Secretary challenges in this case: it is theoretically possible that someone will see how a voter voted. The key to preventing the theoretical possibility from becoming an actual problem is to implement the appropriate processes with the appropriate safeguards to ensure that the highest levels of integrity and confidence are achieved.

Because there are so many possible violations of the secrecy of the ballot, and because no election method is immune from potential breaches of ballot secrecy, a statutory violation cannot reasonably be premised on mere speculation that something theoretically could have happened in an election to violate ballot secrecy – for example, that mail ballots held in a Post Office Box could potentially have been viewed by a postal employee or by a union official who had access to the box, or that security cameras hidden in the ceiling of a room in which voting occurred could potentially have been used to spy on voters. *See, e.g., Hodgson v. Local Union No. 920, Int'l Bdh. of Teamsters*, 327 F. Supp. 1284, 1285-86, 1287-88 (E.D. Texas 1971) (no statutory violation where ballots were locked in vault overnight); *cf. Dole v. Graphic Communications Int'l Union*, 722 F. Supp. 782, 785-86 (D.D.C. 1989) (union violated LMRDA by refusing – presumably on ballot secrecy grounds – to count mail ballots that had been collected by union stewards, who had paid voters to turn ballots over to them rather than mail them in themselves, and who had subsequently mailed the ballots in bulk).

Rather, there must be some showing that ballot secrecy was compromised or that the union failed to take reasonable steps to promote ballot secrecy. *See, e.g., Marshall v. Local Union 12447, United Steelworkers*, 591 F.2d at 205 (finding violation in union's failure to instruct voters to use voting boxes on tables to shield their ballots while voting and to limit number of voters given ballots at any one time to the number of available boxes, because such "measures, which were neither expensive nor difficult, could have been taken to ensure that each voter marked his ballot in secrecy"); *Brennan v. Local 3489, United Steelworkers*, 520 F.2d at 522 (violation found under similar circumstances and "[t]here was no encouragement of any members to take steps to prevent others from seeing their ballots").

Historically, in all methods of union balloting, some level of trust has been conveyed to disinterested third parties. Whether they are poll workers assisting voters with processing scanned ballots and thus potentially able to see how voters voted, postal workers receiving and holding mail-in ballots, or engineering personnel who support electronic voting systems, there have always been some small number of persons within the election process who could possibly connect a voter with his or her vote. Conveyance of trust to disinterested third parties has been made on the basis of personal oaths, organizational covenants, or contractual obligations.

The Secretary additionally points to procedures to prevent violations of secrecy in mail-ballot and on-site voting. Secretary's Brief at 24. But there is no claim that these procedures are either foolproof or complete. There are many documented cases from on-site and mail-ballot elections where secrecy has been compromised. *See, e.g., Marshall v. Local Union 12447, United Steelworkers*, 591 F.2d at 203-05; *Brennan v. Local 3489, United Steelworkers*, 520 F.2d at 521-22; *Donovan v. CSEA Local Union 1000, AFSCME*, 594 F. Supp. 188, 195-97 (N.D.N.Y. 1984), *aff'd*

in other part and rev'd in other part, 761 F.2d 870 (2d Cir. 1985); *Donovan v. Local Union 887, United Rubber Workers*, 111 L.R.R.M. at 2737 (M.D. Ga. 1982).

All election methods must be based upon prudent practices that have been applied in the form of controls that guard against ill intent, guard against carelessness, provide separation of responsibilities, provide protection of confidential information, prevent or identify misuse and abuse, provide a record to allow independent review and scrutiny, and provide accountability. Further, all election methods must provide adequate safeguards to ensure confidentiality, anonymity, integrity, and secrecy. All election methods must balance the various requirements and objectives of the law so as to fulfill the statutory intent. The issue in ensuring ballot secrecy is not the method of voting, but whether there are appropriate safeguards. That is, the existence and proper execution of the safeguards applicable to a particular method of conducting the election is the critical issue.

II. TECHNOLOGICAL INNOVATION SHOULD NOT BE STIFLED

There can be no dispute that there are significant advantages to electronic voting over mail and on-site voting. For instance, union members who travel frequently, such as airline employees, are able to use any computer or telephone interchangeably to vote at their convenience. Voters can be afforded the option of changing their vote, perhaps reflecting new knowledge or understanding obtained during the voting period. The final vote count is virtually instantaneous and far less costly than in paper-based elections. And the vote is not susceptible to manipulation by misreading ambiguous indications of the voter's intent, as can occur with paper ballots, resulting in miscounted or rejected votes.

All of these and other positive features of electronic voting can be retained while at the same time ensuring ballot secrecy. The Court should not rule in a way that would prevent electronic voting and stifle technological innovation.

The Secretary argues that individuals had access to APA members' EINs and PINs, and could have logged onto the Internet and viewed how members voted. Secretary's Brief at 31. For the reasons explained in Part I, the theoretical possibility that this could occur does not constitute a violation. Moreover, any ruling of the Court should not preclude the possibility that additional safeguards can cure any potential secrecy problem in electronic elections. The mail-balloting procedures promulgated by the Department of Labor came into existence only through a similar evolutionary process.

The current BallotPoint system fully complies with all election requirements of the Labor Management Reporting and Disclosure Act ("LMRDA"), including the requirement that elections be conducted by a secret ballot. But Allied Union Services has taken steps to provide further assurance of secrecy.

For instance, Allied Union Services is in the process of implementing a new version of its BallotPoint electronic voting system that will generate a unique, randomized Voter Identification Number ("VIN") and confidential Personal Identification Number ("PIN") for every potential voter and require that *every member must change his or her PIN prior to voting for the first time*. Feldkamp Amicus Dec., ¶15. Setting the PIN will not be optional and will be required prior to accessing the system. This safeguard has one immediate, enormous benefit: neither the printing contractor that prints voter-login information sent to voters (if such a contractor is used) nor the union staff that assists in conducting the electronic election are able to log in under the guise of a given member, and view or change a vote previously cast by that member. If someone other than the member logs in and sets the PIN prior to the member's attempt to do so, the member will be unable to log in using the login information contained in his or her printed voter documents, and will be immediately alerted that there is a problem, which can then be investigated. Forcing the member

to set the PIN means that the PIN is known *only* to the member and, theoretically, to the voting system's engineering support staff.

As discussed in Part I, the possibility that disinterested persons such as engineering support staff could theoretically see how a voter voted should not be a sufficient basis for finding a ballot secrecy violation, any more so than it would be in the case of a disinterested postal worker with access to the Post Office Box to which mail ballots are returned. However, there is a way to improve ballot secrecy with electronic voting for which there is no equivalent in mail balloting. Specifically, it is possible to separate any information that could be used to identify a voter with the content of his or her vote in such a way that no single person – including a member of the engineering support staff – has access to both the voter's identity and the ballot choices made by that voter. This protection is superior to what can be achieved for ballots residing at the Post Office, where the name of the voter is on the outer envelope, and the content of the vote is readily accessed within the envelope.

Allied Union Services's new BallotPoint system definitively separates the identity of the voter from the contents of the vote by using two computer systems, one of which holds voter-identity information, and the other of which records the votes. Feldkamp Amicus Dec., ¶17. The two systems communicate via a secure Internet channel. The system employs a unique, randomized VIN to tag information passed between computers regarding a particular voter. The vote-recording computer knows this VIN and the vote-content, but not the identity of the voter. The voter-identity computer knows this VIN and the voter's identity, but not the content of the vote. A very restrictive operating protocol prohibits the transfer of a VIN along with any voter's personal identity or vote-content. *Id.*

The number of engineering support staff members for either of the computers is strictly limited, and no one has login privileges to the operating systems of both computers. *Id.* Thus, no single person – even a member of Allied Union Services's staff – can link a voter to his or her vote. Rather, the only way to violate ballot secrecy would require two or more engineering support staff members to conspire with each other. This provides a superior safeguard to that available for mail ballots returned to a Post Office Box, where a single person can violate secrecy. To stay in step with the new technology, Allied Union Services's contracts will proscribe persons with access to either voter identifying information or votes from sharing this information. Indeed, as a third-party election vendor that depends on its integrity to obtain business, Allied Union Services has an incredibly strong interest in not sharing such information. The above described system provides separation between the identity of a voter and the contents of the vote, yet still provides for the retention of sufficient information to delete the votes of voters who become ineligible during the course of an election, and to allow a voter (and only that voter) to change his or her vote.

As an additional safeguard accessible to members, the new BallotPoint system will provide a means whereby every member can view a log of the dates and times of all logins, PIN changes, and votes that have occurred on that member's account. *Id.*, ¶16. This permits each voter to monitor activity on his or her account for any irregularities and readily identify any unauthorized access.

Although the BallotPoint system has at all times fully complied with all election requirements of the LMRDA, innovations like those described above are continually evolving to make electronic voting even more secure. There can be no question that electronic voting can fulfill the ballot secrecy requirements of a union election. The Department of Labor's publication "Conducting Local Union Officer Elections" provides step-by-step instructions for on-site and mail-ballot elections, but says nothing about telephone or Internet elections. To date, providers of such advanced technology

have had to do the best they can, without guidance from the Secretary. Allied Union Services respectfully submits that, if the Court were to sustain the Secretary's position in this case, the Court should narrow its decision to the facts of this case, rather than broadly addressing electronic voting in general. Discouraging the use of valuable technology and chilling further technological development in this area should be avoided. Balancing the requirements of the LMRDA is delicate and difficult to achieve. The test is not the method of the election, but the execution of the election process. A properly designed methodology for electronic voting is not only as good as on-site and mail-ballot approaches, but is superior to those methods. The Court should not stunt the growth of Internet and telephone voting.

CONCLUSION

For the above reasons, the Secretary's Motion for Summary Judgment should be denied.

Respectfully submitted,

/s/ Yona Rozen

YONA ROZEN (State Bar No. 17358500)
Gillespie, Rozen, Watsky,
Motley & Jones, PC
3402 Oak Grove Ave. Suite 200
Dallas, Texas, 75204
Phone: (214) 720-2009
Fax: (214) 720-2291

JEFFREY B. DEMAIN, *pro hac vice application pending*
(California State Bar No. 126715)
JONATHAN WEISSGLASS, *pro hac vice application pending*
(California State Bar No. 185008)
Altshuler, Berzon, Nussbaum,
Rubin & Demain
177 Post Street, Suite 300
San Francisco, CA 94108
Phone: (415) 421-7151
Fax: (415) 362-8064